IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A semiconductor integrated circuit device comprising:

a first ~~memory~~ RAM for inputting and outputting data between a bus and itself;

a second ~~memory~~ RAM for inputting and outputting data between the bus and itself;

a secret key holder for holding a secret key;

a bus port for controlling access from outside to the bus;

a CPU for storing an encrypted program and a decryption program in the first memory RAM via the bus port, decrypting the encrypted program by using the decryption program and the secret key, and executing the decrypted program; and

a controller for causing~~, when the encrypted program and the decryption program are stored in the first memory,~~ the bus port to disable access from the outside[[,]] and ~~enabling~~ enable access to the first and second ~~memories~~ RAMs when the encrypted program and the decryption program are stored in the first RAM, ~~and~~ thereby transferring the encrypted program and the decryption program from the first ~~memory~~ RAM to the second ~~memory~~ RAM,

disabling access to the first ~~memory~~ RAM when the transfer is completed, and

disabling access to the second ~~memory~~ RAM when the decryption and the execution of the decrypted program are completed.

2. (Original) The semiconductor integrated circuit device of claim 1, further comprising:

a secret key access port for controlling access from the CPU to the secret key holder, wherein

the secret key access port enables access to the secret key holder when the transfer is completed and disables access to the secrete key holder when the execution of the decrypted program is completed.

3. (Original) The semiconductor integrated circuit device of claim 1, wherein the CPU includes a register and erases data stored in the register if the execution of the decrypted program is completed.

4. (Currently Amended) The semiconductor integrated circuit device of claim 1, wherein the controller controls access to the first and second ~~memories~~ RAMs by controlling chip select signals to the first and second ~~memories~~ RAMs.

5. (Currently Amended) The semiconductor integrated circuit device of claim 1, wherein

the controller includes a flag storing portion for storing first and second flags, enables access to the first and second ~~memories~~ RAMs when the first flag is set, disables access to the first ~~memory~~ RAMs when the first flag is reset and the second flag is set, and disables access to the second ~~memory~~ RAMs when each of the first and second flags is reset,

the bus port disables access from the outside when at least one of the first and second flags is set, and

the CPU sets the first and second flags when the encrypted program and the decryption program are inputted to the first ~~memory~~ RAM, resets the first flag when the transfer is completed, and resets the second flag when the execution of the decrypted program is completed.

6. (Currently Amended) A semiconductor integrated circuit device comprising:

a first ~~memory~~ RAM for inputting and outputting data between a bus and itself;

a second ~~memory~~ RAM for inputting and outputting data between the bus and itself;

a first ~~memory~~ RAM port connected between the bus and the first ~~memory~~ RAM to control access from the bus to the first ~~memory~~ RAM;

a second ~~memory~~ RAM port connected between the bus and the second ~~memory~~ RAM to control access from the bus to the second ~~memory~~ RAM;

a secret key holder for holding a secret key;

a bus port for controlling access from outside to the bus;

a CPU having a register, the CPU writing an encrypted program and a decryption program in the first ~~memory~~ RAM via the bus port, decrypting the encrypted program by using the decryption program and the secret key, writing the decrypted program in the second ~~memory~~ RAM, and executing the decrypted program; and

a controller for causing~~, when the writing to the first memory is completed,~~ the bus port to disable access from the outside to the bus, ~~causing~~ the first ~~memory~~ RAM port to disable the writing to the first ~~memory~~ RAM, and ~~causing~~ the second ~~memory~~ RAM port to enable access to the second ~~memory~~ RAM when the writing to the first memory is completed and

causing, when the execution of the decrypted program is completed, the CPU to erase data stored in the register and disable access to the secrete key holder, while causing the second ~~memory~~ RAM port to disable access to the second ~~memory~~ RAM.

7. (Currently Amended) A semiconductor integrated circuit device comprising:

a first ~~memory~~ RAM for inputting and outputting data between a bus and itself;

a second ~~memory~~ RAM for inputting and outputting data between the bus and itself;

a ~~memory~~ RAM port connected between the bus and the first memory to control access from the bus to the first ~~memory~~ RAM;

a secret key holder for holding a secret key;

a bus port for controlling access from outside to the bus;

a CPU having a register, the CPU writing an encrypted program and a decryption program in the first ~~memory~~ RAM via the bus port, decrypting the encrypted program by using the decryption program and the secret key, writing the decrypted program in the second ~~memory~~ RAM, and executing the decrypted program; and

a controller including a ~~memory~~ RAM initializer for erasing data in the second ~~memory~~ RAM, the controller causing, when the wiring to the first ~~memory~~ RAM is completed, the bus port to disable access from the outside to the bus and causing the memory port to disable the writing to the first ~~memory~~ RAM and

causing, when the execution of the decrypted program is completed, the CPU to erase data stored in the register and disable access to the secret key holder and causing the ~~memory~~ RAM initializer to erase the data in the second ~~memory~~ RAM.

8. (Currently Amended) A semiconductor integrated circuit device comprising:

a first ~~memory~~ RAM for inputting and outputting data between a bus and itself;

a second ~~memory~~ RAM for inputting and outputting data between the bus and itself;

a secret key holder for holding a secret key;

a decryption key holder for holding a decryption key;

a bus port for controlling access from outside to the bus;

a CPU including a register, the CPU performing first storage for storing the encrypted decryption key and a decryption key decryption program in the first ~~memory~~ RAM via the bus port, performing first decryption for decrypting the encrypted decryption key by using the decryption key decryption program and the secret key, writing the decrypted decryption key in the decryption key holder, performing second storage for storing an encrypted program and a

decryption program in the first ~~memory~~ RAM, performing decryption for decrypting the encrypted program by using the decryption program and the decrypted decryption key, and executing the decrypted program; and

a controller for causing, when the first storage to the first ~~memory~~ RAM is completed, the bus port to disable access from the outside to the bus and enabling access to the first and second ~~memories~~ RAMs such that the encrypted decryption key and the decryption key decryption program are transferred from the first ~~memory~~ RAM to the second ~~memory~~ RAM,

enabling, when the transfer is completed, access to the secret key holder and disabling access to the first ~~memory~~ RAM;

causing, when the first decryption is completed, the CPU to erase data stored in register and disable access to the secret key holder, while disabling access to the second ~~memory~~ RAM, enabling access to the first ~~memory~~ RAM, and causing the bus port to enable access from the outside to the bus,

causing, when the second storage to the first ~~memory~~ RAM is completed, the bus port to disable access from the outside to the bus and enabling access to the second ~~memory~~ RAM such that the encrypted program and the decryption program are transferred from the first ~~memory~~ RAM to the second ~~memory~~ RAM,

enabling, when the transfer is completed, access to the decryption key holder and disabling access to the first ~~memory~~ RAM, and

causing, when the second decryption and the execution of the decrypted program are completed, the CPU to erase data stored in the register and disable access to the secret key holder and disabling access to the second ~~memory~~ RAM.

9. (Withdrawn) A program delivery method for delivering a program between a first device and a second device, the method comprising the steps of:

transferring a public key from the second device to the first device;

transferring a decryption program to the second device from the outside thereof;

encrypting the program by using the public key in the first device and transferring the encrypted program to the second device; and

decrypting the encrypted program by using a secret key corresponding to the public key and the decryption program in the second device.

10. (Withdrawn) A program delivery method for delivering a program between a first device and a second device, the method comprising the steps of:

transferring a public key from the second device to the first device;

encrypting a decryption key by using the public key in the first device and transferring the encrypted decryption key to the second device;

decrypting the encrypted decryption key by using a secret key corresponding to the public key in the second device;

encrypting the program by using an encryption key corresponding to the decryption key in the first device and transferring the encrypted program to the second device; and

decrypting the encrypted program by using the decrypted decryption key in the second device.

11. (Withdrawn) A program delivery system for delivering a program, the system comprising:

a first device and a second device,

the first device encrypting the program by using a public key and transferring the encrypted program to the second device and

the second device decrypting the program encrypted by the first device by using a secret key corresponding to the public key and a decryption program transferred from the outside of the second device.

12. (Withdrawn) A program delivery system for delivering a program, the system comprising:

a first device and a second device,

the first device encrypting a decryption key by using a public key, transferring the encrypted decryption key to the second device, encrypting the program by using an encryption key corresponding to the decryption key, and transferring the encrypted program to the second device,

the second device decrypting the decryption key encrypted by the first device by using a secret key corresponding to the public key and decrypting the program encrypted by the first device by using the decrypted decryption key.